Internet of Things

Fog Computing and Aggregation

By Robert P. Smith II

bob@rpsmith.net www.rpsmith.blog

By 2020, Gartner's latest estimates indicate over 20 billion deployed Internet of Things (IoT) devices. Many factors will impact reaching these numbers. Significant design and engineering advances are redefining traditional network - compute paradigms, or depending on your age, resurfacing old ones. Read how key drivers will shape the newest Internet 'it-technology.'

IoT Units Installed Base by Category (Millions of Units)

Category	2016	2017	2018	2020	16-20 GAGR
Consumer	3,963.0	5,244.3	7,036.3	12,863.0	34.22%
Business: Cross-Industry	1,102.1	1,501.0	2,132.6	4,381.4	41.20%
Business: Vertical-Specific	1,316.6	1,635.4	2,027.7	3,171.0	24.58%
Grand Total	6,381.8	8,380.6	11,196.6	20,415.4	33.74%

Source: Gartner (January 2017)

Telematics

Insatiable demand for data and remote control applications will deliver these numbers. IoT devices are designed covering three primary functions.

- *Sensors measure the environment. They can be simple like a thermometer measuring temperature; or more complex like soil moisture and pH measurements.*
- *Actuators* perform electro-mechanical tasks. The circuit that starts the heater or air conditioner in a thermostat is a simple example.
- *Compute-Analytic Platforms* intake sensor measurements, record them for analysis and can command actuators reacting sensor measurements. Basic thermostats combine

these three functions - sense temperature, at a programmed setting activate heating or air conditioning.

Together, these functions are *Telematics*.

The Cloud

Telematics relies on the *Cloud*. *On-demand* scalability to meet the gargantuan amount of data generated makes cloud services ideally suited for IoT applications. Since data has no value without insights and decisions, another area where the cloud excels is scalability to meet computational demands. Cloud data centers located on major networks and highly secure make them über-economic and reliable.

The Fog

As fog is just a cloud close to the ground so the metaphor extends to the IoT world. Low power and inexpensive computers allow the option of local telematics. Not all data needs to be stored nor decisions need to take place in cloud centers. If so, it isn't practical to burden the cloud and feeder networks. *Fog aggregation and computing,* as the terms suggest, takes tasks normally associated and performed in the cloud but executes them locally without transmission over the Internet.

A perfect example is the FitBit, a *wearable* IoT device that measures steps taken. The device includes a display providing the user instant updates and analytics converting data to preferred indicators like miles walked. For many, this telematic operation is all they use the FitBit for. Breaking this down:

Sense: *steps taken,*
Decide: *convert to miles and compare to daily goal*
Actuate: *(if not reached) walk more*

Fitbit provides cloud services combining other telematics, like weight, from their IoT scale, Aria, to drive richer insights. For many of their users, all they seek from FitBit is steps taken measurements. This renders cloud services unnecessary because all telematic value is extracted locally from the device. Therefore, there's no reason to transmit, store or analyze the data in the cloud.

General telematic applications like environmental sense and control, inventory management, security and crowd control will drive the cross-industry 41% compound annual growth rate (CAGR) predicted by Gartner. Advances in energy and security needs will drive many applications to the Fog.

Energy

Energy will pace IoT telematics expansion. Sensors and actuators must communicate to be of any value. Wireless sensors make sensor installation fast and easy, but radios that communicate over the Internet use a lot of energy. Radio protocols, like IPv6 over Low power

Wireless Personal Area Networks (6LoWPAN) and Bluetooth Low Energy (BLE) allowing ultra low energy communications over distances as far as 40km.

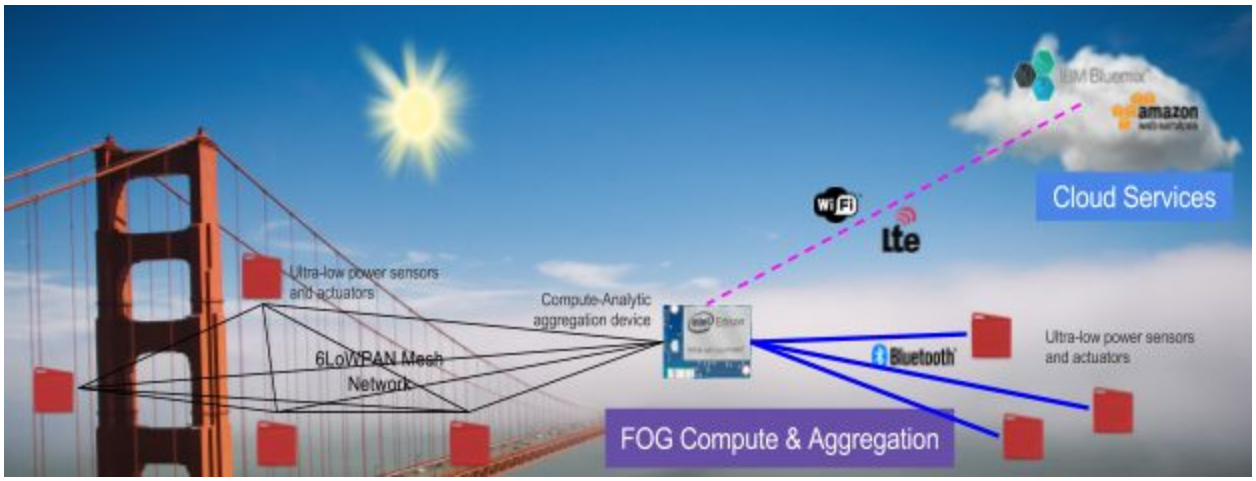
Energy requirements of these devices are so low, they can absorb the energy needed from their surroundings called Energy Harvesting. This is not a new concept, solar and wind power are familiar examples. Advances in the technology now collect and convert artificial sources like broadcast radio waves and natural phenomenon like the Earth's magnetic resonance into small amounts but useful energy. This technology is ideal for Fog based sensor and actuator networks.

Security

Of particular concern with IoT Internet-connected applications and their legions of devices is infiltration by hackers. A popular exploit is pressing many devices into service with a virus dormant until called to execute in unison. A common tactic is to have all devices attach a particular website. The inrush of connect requests overwhelms the site effectively shutting it down. Called Denial of Service (DoS) attacks, when many devices over a wide area are used, Distributed is added making it a DDoS attack.

IoT devices are a favorite because they are thought to be mostly inert and simple. On the contrary, many IoT devices are more than capable of hosting, spreading and acting on these viruses. Internet-connected IoT devices were recently drafted into service working to attack key Internet facilities causing a ruckus. Internet-connected IoT disruption need not be deliberate. A bad line of code can cause many devices to 'phone home' at once causing unintended mischief.

Sensors and actuators on low energy wireless Fog networks aren't directly connected to the Internet. Instead, they aggregate through compute-analytic processors that may or may not be connected to the Internet. This won't one-hundred-percent lock out all Fog connected devices from exploits, but the barrier calls for extra effort hackers will invest elsewhere.



In conclusion, the Fog is an important architectural aspect in telematic applications, particularly when many devices, real-time tasks and low power are required.